在移动战术环境下的终端安全接入方案 *

秦秋阳，江凌云†

(南京邮电大学 通信与信息工程学院，南京 210003)

摘 要：针对在搜索、救援、军事作战等环境中，恶劣的通信状况和频繁的终端移动造成传统的安全认证体制难以实现终端的安全接入的问题，提出了一种移动战术环境下的终端安全接入方案。该方案采用一种无证书的密钥管理机制，分析了终端移动后的安全认证过程，以及终端和网关受损或被入侵后的安全处理方法。仿真结果表明，该方案提高了网关与终端之间授权与认证的安全性，能够很好地抵抗已知攻击，解决了战术环境下缺少相互认证以及密钥托管的问题，并且该方案使用的无证书密钥算法较其他算法有更好的安全性和更少的计算开销，可以对终端移动过程中接入网关的安全性与能耗进行权衡。

关键词：战术环境；终端安全接入；无证书密钥管理；物联网安全

中图分类号：TP391 doi: 10.19734/j.issn.1001-3695.2020.04.0073

Secure access scheme for terminals in mobile tactic environment

Qin Qiuyang, Jiang Lingyun†

(*College of Telecommunications & Information Engineering*, *Nanjing University of Posts & Telecommunication*, *Nanjing* 210003, *China*)

Abstract: Poor communication conditions and frequent terminal movements in search, rescue, military and other environments make it difficult for traditional security authentication systems to achieve secure access to terminals. To solve this problem, this paper proposed a scheme about security connection with terminals in the mobile tactical environment. This scheme used a certificateless key management mechanism to analyze the security authentication process after the terminals were moved and the secure processing method after terminals and gateways were damaged or invaded. Simulation results show that the scheme improves the security of authorization and authentication between the gateway and the terminal, can well resist some known attacks, solves the problem of lack of mutual authentication and key escrow in the tactical environment, and the certificateess key algorithm used in this sheme has better security and less computational overhead than other algorithms, and can balance the security of accessing a gateway with energy consumption during a terminal movement.

Key words: tactical environment; secure terminal access; certificateless key management; Internet of Things security

0 引言

与传统互联网相比，物联网将网络世界扩展到物理世界，由此产生了一些更复杂的新安全问题[1]。物联网面临着设备资源限制、终端高移动性、攻击更加多样、认证尚未标准化等诸多安全挑战，这使得在物联网中保障消息的机密性完整性、身份验证过程的安全性、用户信息的隐私性等要求的满足存在更多隐患[2]。

民用物联网系统中一些现有的安全问题通过一些方案得到了有效的解决，这些方案包括密钥认证体制、数据标签、IP 回溯法、基于软件定义网络(SDN)的安全方案等[2]。民用物联网系统通常拥有稳定的网络连接，而在战术环境中，情况更加复杂，网络连接不稳定。

在搜索、救援以及军事作战等战术环境中，障碍物较多、敌人打击、云端距离较远等因素使得该环境下的网络信号变动较大，人们时常需要处理通信中断、间断和受限(DIL)的网络环境[3]。此外，战术环境中还可能存在动态的上下文、更有限的计算资源、终端和网关受损或被入侵等问题[4]，所以需要时刻监视终端和网关的安全状况，及时发现可能发生的安全问题，并采取有效措施。战术环境下的终端具有更高的移动性，所以在终端移动过程中，需要保证已被授权的终端的验证信息能够高效安全地迁入到该终端即将接入的边缘网关[5]。

现有的战术环境下的终端安全接入方案考虑不够全面，主要实现的是终端接入网关的授权，和网关信息迁移后终端重新接入网关的认证过程，并没有详细考虑终端和网关受损或被入侵的解决方案。而且这些方案仍然存在安全隐患，如终端接入网关的过程缺少相互验证，缺少信任托管等。

无证书的密钥算法很好地解决了上述安全问题，该算法最早由 Riyami 等在文献[6]中提出，后来经过不断优化[7~10]，这种方案已经能够较好地抵抗多种已知攻击。

1 相关工作

目前，国内外一些学者已经提出了许多关于终端安全接入的方案与算法。在常规的环境中，文献[11]提出了基于椭圆曲线加密(ECC)算法[12]的终端与服务器之间的安全认证方案，随后文献[13]中指出该方案无法实现相互认证，并改进了该方案。文献[14]又指出文献[13]的方案仍然不安全，并在此基础上继续改进。但是上述方案算法都是基于正常的物联网环境，战术环境中的验证方案有较大不同。

在复杂战术环境中，文献[15]结合标识密码体系(IBC)[16,17]与无可信第三方(TTP)[18]的安全密钥协议，在节点与云端失去连接的情况下，实现了终端安全接入边缘网关的目的。但是该文献与后续文献[19]的认证接入方法不能保证信任托管和终端与网关的相互认证。且在文献中采取完全相

收稿日期：2020-04-02；修回日期：2020-05-23 基金项目：国家重大科研仪器研制项目(61427801)

作者简介：秦秋阳(1996-)，男，江苏南京人，硕士研究生，主要研究方向为物联网安全；江凌云(1970-)，女(通信作者)，安徽安庆人，副教授，硕导，硕士，主要研究方向为下一代网络(jiangly@njupt.edu.cn).

同的认证方案，该方案要求网关完全信任另一个网关，因此具有较大安全隐患。

在动态网络中，Seung 等人提出了无证书的密钥管理方案[20,21]。该方案可用于解决上文中提到的信任托管问题，在形成加密密钥过程中实现节点之间的相互验证，增强已知攻击的抵抗性。但是该方案中关于节点移动情况的介绍不够充分，对于节点受损或遭到入侵以后的处理工作不够详实。

针对以上文献存在的问题，本文继续沿用文献[15]的战术环境，引入主控节点的概念，结合无证书的密钥管理方案，解决缺少信任托管以及相互认证的问题，并详细分析动态战术网络中终端移动后的安全认证过程，讨论终端和网关受损或被入侵的处理方法。

2　战术环境下的网络拓扑结构

本文中战术环境的网络拓扑结构如图 1 所示。由于战术环境情况较为复杂，通信质量不佳，该环境下的节点可能随时与云端断开连接。在本文考虑的战术模型中，节点与云端断开连接，此时网络中主要存在三种节点，分别是终端、边缘网关以及主控节点。

在具体的战术环境中，士兵或无人车、无人机等机器都会携带多种传感、执行设备以及一部 Android 客户端，该 Android 客户端就是终端，所有设备会与客户端相连接，并传递数据，它可对设备的数据进行收集以及简单处理。终端不断移动，并与边缘网关相连，终端可以从网关获取更多服务，同时网关也向终端发布命令。图 1 中箭头表示终端移动方向，它们可以在所连接网关的信号范围内移动，也可能移动到其他网关的信号范围。

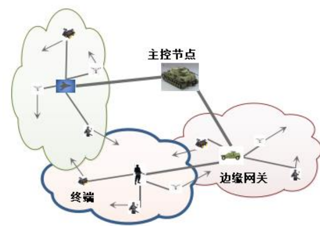


图 1　战术环境的网络拓扑

Fig. 1　Network topology diagram of tactical environment

网关可以是一台具有较强数据处理能力和信号接收能力的计算设备，由每个班组中的固定人员携带，或者装备在一辆较大的无人车或无人机上。图 1 中网关都有自己的信号可传达范围，每个网关通过单跳或多跳的方式连接到主控节点。考虑到相对于终端，网关运动范围较小、运动次数较少，且网关的运动可以等价于终端的相对运动，所以本文只考虑终端的运动情况。

在所有的网关中选取一个处理能力大、移动性小的网关作为主控节点，如临时指挥所或大型的战车。主控节点一般静止不动，或移动性很小，它的主要用于：在其他所有节点部署到具体环境之前，为它们生成系统参数，该参数用于这些节点以后相互验证以及形成配对密钥；在系统运行过程中，利用其较完善的入侵检测机制，发现某些受入侵或受损的节点；对所有数据进行汇总并向其他节点发布命令。

3　基于无证书密钥管理的终端接入方案

在 DIL 战术环境中，终端、网关之间需要形成配对密钥并验证对方是否可信。终端在不断移动的过程中，会从原先所在的网关信号覆盖范围转移到另一个网关信号覆盖范围。终端移动后，会连接到新的网关，因此需要将原网关中已处理的信息安全地迁移到新网关。此外，由于 DIL 战术环境较为复杂，可能会出现通信中断、终端损坏以及终端移动出网关信号范围却没有告知网关的情况。而且，若某个网关受损，该网关下的所有终端需要安全地连接到新的可连接的网关。本节将会对以上所有情况进行详细说明并提出处理方法。

3.1　节点之间相互验证

节点之间相互验证存在三种情况，分别是终端与终端之间，终端与网关之间，网关与网关之间，由于这三种情况的验证方法相类似，所以本节主要针对终端与网关之间建立相互信任关系进行详细介绍。终端安全接入网关分为两个步骤，首先终端需要和网关形成配对密钥，而在形成配对密钥的过程中，双方会进行互相验证；随后网关会通过终端发送的设备 ID 生成 BLS 证书[22]，该证书可用于后续终端移动后接入其他网关的验证。

3.1.1 生成公钥、私钥与个体密钥

基于无证书密钥管理的方案，在节点部署到战术环境之前，每个节点需要接收系统参数，具体过程参考文献[21]。主控节点的密钥生成中心 (KGC) 生成系统参数 $\Omega=\{F_q, E/E_q, G_q, P, P_{pub}=xP, h_0, h_1, h_2, h_3\}$ 以及完全保密的密钥 x。其中 F_q 表示包含 q 个元素的有限域(其中 q 有 k-bits)；E/F_q 表示有限域 F_q 上椭圆曲线 E 的所有有理点组成的集合；G_q 表示椭圆曲线的加性环组；P 为 G_q 中某一点；P_{pub} 为 KGC 生成的系统公钥；h_0，h_1，h_2，h_3 分别为四种形式的哈希函数；x 为主控节点生成的主私钥，其中 $x\in_R Z_q^*$，$_R Z_q^*$为 整数乘法组(模 q)。主控节点公布 Ω，保密 x。

主控节点为每个网关以及终端分配一个特殊标识符，其中某网关 n_B 标识符为 B，某终端n_A 标识符为 A。终端可通过蓝牙或 Wi-Fi 等无线连接方式与网关连接。终端与网关通过主控节点提供的系统参数以及标识符生成各自的公钥与私钥。因为终端与网关生成密钥步骤相同，这里只介绍终端 n_A 的密钥生成。图 2 是终端节点 A 完整私钥、完整公钥以及个体密钥生成过程。

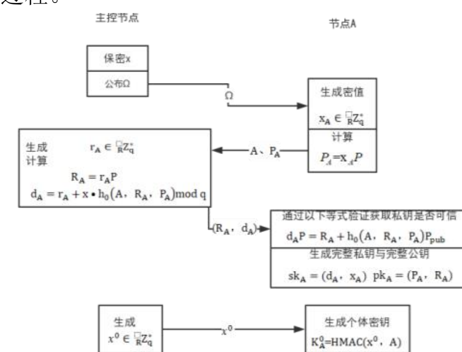


图 2　终端节点公钥、私钥以及个体密钥生成过程

Fig. 2　Generation process of end node public key, private key and individual key

3.1.2 生成配对密钥

在所有终端与网关生成私钥、公钥以及个体密钥以后，需要将它们部署到战术环境中。而在节点部署完成以后，所有可通信节点之间都需要生成配对密钥。但是一般情况下，终端只能同时与一个网关进行连接，所以只能同时与一个网关形成配对密钥。

任意的终端或网关都会向周围广播自己的标识符和公钥，当 n_A 接收到来自 n_B 的广播以后，通过以下过程两者建立长期主配对密钥 K_{AB} 以及加密配对密钥 k_{AB}，具体过程如图 3 所示。

因为只有拥有系统参数的两个节点才能完成以上步骤，所以上述方案既可以在任意两个节点之间形成用于加密通信的配对密钥，也可以验证建立密钥的两个节点是否可信。此外，由于生成主配对密钥需要通过 ECC 算法，该算法的计算是无证书密钥方案的主要耗能过程，但是保持配对密钥始终不变可能对安全性产生影响，所以可以周期性地更新加密密

钥，并保持主配对密钥不变。

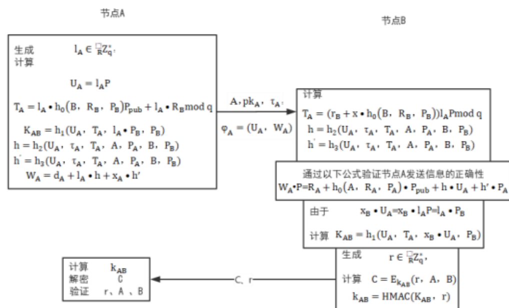


图 3　节点之间配对密钥的生成过程

Fig. 3　Generation process of pairing keys between nodes

3.1.3 生成 BLS 证书

通过第一步验证后，终端提供其设备 ID 作为设备公钥，文献[6,15]中选取可获得的 Android 设备 ID，该 ID 在节点部署完成之前随机生成。网关获取设备 ID 后为终端生成 BLS 证书[22]。BLS 证书是由网关使用终端的设备 ID、网关的设备 ID 以及私钥生成，它将保存在网关内，之后该网关发送设备 BLS 证书以及网关设备 ID 给终端。

在终端与网关通信的过程中，双方使用加密密钥加密并发送信息。为增强安全性，终端向网关请求服务之前需要发送设备 ID 以及 BLS 证书，网关验证 BLS 证书的正确性以后会发送网关设备 ID 供终端核实。

通过以上两个步骤，终端与网关之间完全建立信任关系。网关通过个体密钥向主控节点发送消息，告知主控节点有关该终端的信息。

建立网关和网关之间的信任关系的步骤与上述验证过程相同。而对于建立终端与终端的之间信任关系，因为终端与终端之间不需要相互提供服务，所以只需要两者之间建立配对密钥，并不需要生成 BLS 证书。

3.2　节点移动后的安全认证

在战术环境中，终端始终在变化位置，而网关信号所覆盖的范围是有限的，所以终端可能从原先所连接的网关信号覆盖的区域移动到其他区域，这时终端与当前所属网关不能继续通信。而终端需要继续连接其他网关，让其他网关提供终端所需的相关服务。但是考虑到终端与接入的网关之间建立完整的信任关系较为复杂，需要消耗较多的能量，所以终端移动后接入的网关可以与原先所属网关通信，请求原所属网关发送终端的信息给移动后网关，减少终端再次安全认证的能量损耗。为了以下表述方便，分别将终端当前所属网关命名为 CA，移动后连接的网关命名为 CB。

3.2.1 终端和网关断开连接

终端移动主要分为两种情况，分别是终端主动向 CA 提交离开请求；以及终端突然与 CA 毫无预兆地断开连接。具体的处理情况如图 4 所示。



图 4　终端与所属网关 CA 断开连接后的处理过程

Fig. 4　Processing procedure of the terminal is disconnected from its own gateway CA

具体解释为：由于复杂的战术环境，可能存在通信信号不佳、终端被入侵、终端设备受损或丢失等情况，此时终端未向网关提交申请就断开连接。预先设置一个较大的时间值 Tm，若该终端超过 Tm 时间未与新的网关连接，即 CA 没有收到其他网关需要该终端信息的申请(3.2.2 将说明：终端连接新网关 CB，CB 需要向 CA 申请获取该终端信息)，或该终端没有重新连接 CA，则判定该终端已经完全受损或遭到入侵，CA 向主控节点汇报此消息。若在 Tm 时间内终端重新连接 CA，这可能是由于通信不佳而造成的间断性失联，可以预先设置较短的时间值 t，如果终端与 CA 断联的时间不超过该时间值 t，终端需要再次连接，CA 只要求获取终端的 BLS 证书，并且两者之间重新生成加密密钥；如果断连时间超过 t，终端需要再次连接，必须与 CA 重新形成完整的配对密钥。在终端重新连接 CA 后，CA 向主控节点提交此次事件信息。若 Tm 时间内终端连接其他网关，则参照 3.2.2 节：终端与新网关连接的验证过程。

如果终端主动向 CA 提交离开申请，但是当超过时间值 Tm 后，终端没有连接新的网关，则判断该终端已经受损或被入侵，CA 向主控节点报告该消息。若该终端在时间 Tm 内重新与 CA 连接，则判断终端断连的时间是否超过预设的时间值 Tn(Tm>Tn)，若超过，两者需要重新生成完整的配对密钥；否则只需要生成加密密钥并认证 BLS 证书。若该终端在 Tm 时间内需要连接其他网关，则参考 3.2.2 的验证过程。

每次验证通过以后，网关都需要通过个体密钥向主控节点提交新连接终端的信息。如果终端或网关的验证不通过，对方要告知主控节点该消息。

3.2.2 终端移动后连接网关

当终端通过加密密钥向 CA 主动提交离开申请，CA 会在数据库列表中记录下该终端的状态，以及它的所有证书、密钥以及数据信息，并向主控节点提交该终端离开的消息。当终端来到 CB 的信号覆盖区域，并向 CB 申请连接，需要与 CB 之间建立完全的信任关系，而为了节省时间、减少能量损耗，可以通过如图 5 所示验证过程完成。

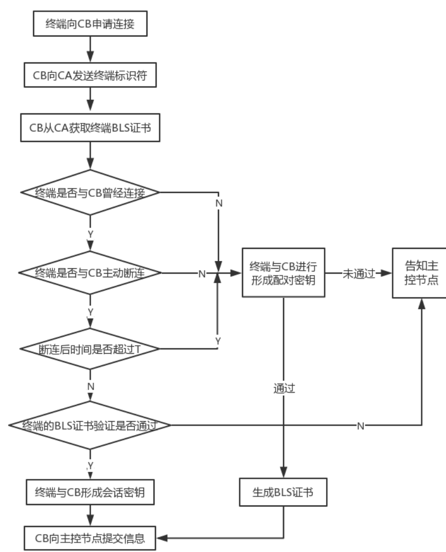


图 5　终端申请加入 CB 的验证过程

Fig. 5　Verification process of the terminal applying to join CB

该情况的具体步骤如下：终端与 CB 通过无线方式连接，并向 CB 发送 CA 的标识符。CB 与 CA 通过加密密钥相互通信(该步骤是前提，它要求 CB 与 CA 两个网关之间已经建立完全的信任关系且能够相互通信)，CB 申请获取该终端的所有相关信息。若终端与 CB 在之前没有过连接，即双方并没有形成过配对密钥，则需要形成完整配对密钥，并且 CB 为终端生成新的 BLS 证书，CB 将新 BLS 证书以及网关设备 ID

发送给终端，最后向主控节点提交该终端接入的信息。若终端与 CB 之前有过通信，且终端与 CB 断开连接时是主动提交离开请求，则判断从断开连接到终端申请接入 CB 的时间是否超过系统设置的时间 T，如果超过该时间，则需要重新生成配对密钥；如果没有超过时间 T，双方只需要根据原有的主配对密钥生成加密密钥，随后终端提供 BLS 证书供 CB 验证(此时 CB 已经从 CA 获取终端的 BLS 证书)，最后 CB 发送网关设备 ID 给终端，终端即可向 CB 要求提供服务。若完成验证，CB 向主控节点提交终端信息。若终端或 CB 发现对方未通过验证，需要向主控节点告知该消息。

3.2.3 边缘网关受损

如果某边缘网关 CA 受损或被入侵，与该网关连接的所有终端需要连接到其他网关，由它们提供服务。主控节点拥有较为强大的计算能力以及入侵检测机制，若发现 CA 受损或遭到入侵，需要告知与 CA 连接的所有终端马上断开与 CA 的连接，并连接到其他网关。

由于战术环境较为复杂，主控节点或许不能将 CA 受损或被入侵的消息通过个体密钥传递给与 CA 连接的所有终端。可以通过图 6 所示过程将该消息告知与 CA 连接的终端。

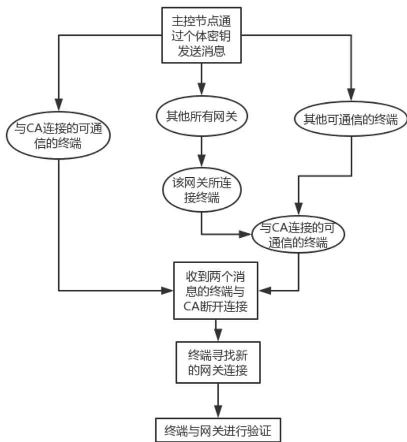


图 6 网关 CA 受损消息的传递过程

Fig. 6 Delivery process of the gateway CA damaged message

具体步骤解释如下：主控节点通个体密钥发送 CA 被入侵的消息给所有主控节点能通信的其他网关和终端。与 CA 连接的终端接收到主控节点的消息以后，立刻切断与 CA 的连接；网关收到消息以后，立刻通过加密密钥将该消息发送给与它相连的所有终端。收到该消息的终端再次通过加密密钥将该消息发送给与它们相连的其他终端。如果与 CA 相连的终端接收到两个及以上 CA 被入侵的消息，这些终端马上与 CA 切断连接。原先与 CA 连接的终端切断连接以后，需要寻找新的网关获取服务，终端与新网关建立连接的验证过程参考 4.1 节所示。

4 安全性分析与性能分析

本节主要分析本文所采用方案的安全性以及性能。从安全性角度分析可知，该方案能够抵抗一些已知攻击，解决了过去战术环境中终端可信接入存在的问题，并且对比了本文的算法较其他无证书密钥算法[22,23]的安全需求。此外，还从性能的角度，分析了本文使用算法的时间与计算量对比其他算法的优势，最后权衡了安全性与能耗、时间之间的关系。

4.1 安全性分析

a)弹性妥协(compromise-reselience)。假设攻击者捕获了某节点，并获取了该节点所有的密钥和证书。因为任意两个节点之间的配对密钥都是相互独立的，所以攻击者不能获得其他节点的密钥和证书。且由于 ECC 的复杂性，攻击者不可能知道主控节点的主私钥 x，所以攻击者不可能影响其他节点之间的通信。

b)抵抗克隆和冒充攻击。如果攻击者捕获了一个节点，则他可以进行克隆攻击。攻击者提取该节点的密钥，并在另一个邻域中复制该节点。此时通过主控节点的入侵检测机制，主控节点发现受损节点以后告知所有节点。若该被入侵节点是网关，参考 4.2.2 即可；若被入侵节点是终端，则主控节点将该消息传递给与该终端连接的网关，网关断开与该节点的连接，并告知主控节点。

攻击者还会使用冒充攻击，直接插入攻击节点与其他节点连接，这样就可能获取网关生成的 BLS 证书，但是由于配对算法的优势，该攻击节点并不能和任何节点建立密钥。因为对于冒充节点 n_A 的攻击节点 n_c，他想要广播标识符后与 n_B 建立配对密钥，但是 n_B 会通过 $W_A \bullet P = R_A + h_0 A$，$R_A$，$P_A ?P_{pub} + h ?U_A + h' ?P_A$ 等式来判断 n_A 合法性，因为 n_A 只有接收到来自主控节点的系统参数 Ω，并通过此参数生成完整公钥，发送给 n_B 的信息才能通过上述等式验证。同理，n_B 只有接收系统参数 Ω，才能计算 d_B，并通过计算 $T_A = d_B \bullet U_A$，才能解封 n_A 的信息。此外，n_c 可能冒充 n_B 随机生成主配对密钥 K_{AB} 与随机数 r，并计算 $C = E_{k_{AB}}(r, A, B)$ 发送给 n_A (其中 $E_{k_{AB}}(m)$是利用密钥 k_{AB} 对消息 m 进行加密的对称密钥加密算法，可反向解密)，n_A 会用 k_{AB} 解密 C。由于 $k_{AB} = HMAC(K_{AB}, r)$ 是由 n_A 和 n_B 分别计算(其中 HMAC[25]为哈希运算消息认证码，使用 x^0 和 A 作为输入，利用哈希运算输出 K_A^0)，且 n_B 不知道 K_{AB}，所以 n_B 不能生成正确的 k_{AB}，则 n_A 不能解密 C，所以 n_C 冒充 n_B 仍会被发现。

c)抵抗“已知密钥”(know-key)攻击。“已知密钥”攻击是指攻击者知道了加密密钥，并提取主配对密钥。由于计算加密密钥算法 HMAC 的单向性，所以攻击者不可能提取成功。而且由于攻击者不知道主密钥，当节点周期性更新加密密钥后，攻击者也不可能知道新的加密密钥。

d)提供互相验证。安全认证步骤中，两个节点之间都有互相验证的过程。第一步通过建立配对密钥验证双方节点，具体的互相验证过程已经在“抵抗克隆和模仿攻击”中阐述。只有当两个节点拥有主控节点发放的系统参数 Ω，双方才能在形成配对密钥过程中通过对方的安全认证并形成密钥。终端在与网关通过无线方式连接时，它将获取网关生成的 BLS 证书以及网关设备 ID，终端每次请求服务时，网关都将验证终端的 BLS 证书，终端也将核实网关的设备 ID。

e)信任托管问题。主控节点发送给终端和网关的系统参数并不是完整的证书，终端和网关需要生成各自的主私钥，根据获取的系统参数 Ω，计算得到完整公钥与完整私钥。由于 ECC 算法的复杂性，任何节点难以获取其他节点的主私钥，也就不能获取其他节点的完整私钥。

表 1 对比了本文方案所使用的的算法与其他两篇参考文献(文献[22,23])提出的无证书密钥算法的安全性对比，其中“√”表示该算法满足对应的安全性需求，“×”表示该方案不满足对应的安全性要求。

表 1 不同算法的安全性对比

Tab. 1 Comparison of security of different algorithms

算法	弹性妥协	克隆冒充	已知密钥	相互验证	信任托管
文献[22]	√	√	√	√	√
文献[23]	×	√	×	√	√
本文	√	√	√	√	√

4.2 性能分析

将本文使用的算法与另外两种无证书密钥管理算法的性能进行比较。首先比较不同算法的计算开销(都使用 160bits 安全级别，其中 T_P 代表 ECC 标量乘法运算所需的时间)，其结果如表 2 所示。

表 2 不同算法的计算开销对比

Tab. 2 Comparison of computational costs of different algorithms

算法	完整密钥	配对密钥	总和
文献[22]	$11T_p$	$15T_p$	$26T_p$
文献[23]	$6T_p$	$7T_p$	$13T_p$
本文	$4T_p$	$9T_p$	$13T_p$

使用 C 语言的大数运算库(MIRACL)实现。在 Windows 7 家庭版，Intel Core i7-4510U CPU @ 2.0 GHz，8 GB RAM，64 位操作系统上运行程序，运算 50 次以后平均计算 T_p 的大小为 1.03ms。图 7 表示不用算法平均耗费时长。

再对不同算法的通信成本进行比较。通信成本主要包括椭圆曲线的大小(设为 e bits)以及发送消息的大小(设为 m bits)，由于三种算法都是基于椭圆曲线的无证书密钥算法，所以通信成本均为 3e+m。

相比于其他两种算法，本文使用算法的通信成本没有改变，但是本文算法的计算开销比文献[22]算法的的计算开销要少 50%，与文献[23]算法的计算开销相当，但是本文算法较文献[23]的算法更安全。

4.3 安全性与能耗权衡

终端移动过程中，会进入新网关的信号范围，并申请与该网关进行连接。如果该终端曾经与此网关生成过配对密钥，并且终端从主动申请与网关断开连接到再次申请连接网关的时间不超过 T，则该终端与网关只需要根据之前生成的主配对密钥计算加密密钥；若该终端断开与网关的连接到重新申请连接的时间超过 T，则需要重新生成完整配对密钥。

预先设置的 T 值越大，那么在一定时间内，终端与网关生成主配对密钥的次数就越少，节点所需要消耗的能量就越少，但是相应的，终端接入的安全性就越低；反之，若 T 值越小，在相同情况下，生成主配对密钥的次数就越多，节点消耗的能量越多，但安全性越高。因此在保证终端接入安全性的同时，需要尽可能地减少能量的损耗，所以本章节主要讨论安全性与能耗之间的权衡。

本小节通过 MATLAB 仿真 random walk mobility model(随机漫步模型)。假设在 400×400m² 的网格空间内，存在均匀分布的 25 个边缘网关，每两个相邻网关之间的距离为 100m，100 个终端随机地分布在此网格中。

在此随机漫步模型中，每个终端首先选取距离它最近的网关进行连接。接下来，该终端每一秒会随机选取上、下、左、右任意方向移动[0，2X] m 的位移(X 为可设置的变量，平均位移值为 X m)。当 X=1 时，仿真的随机漫步模型图 8 所示。

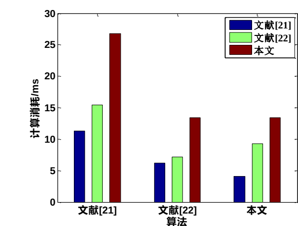


图 7 不同算法计算时间对

Fig. 7 Comparing calculation time of different algorithms

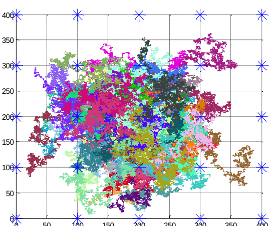


图 8 随机漫步模型仿真

Fig. 8 Simulation diagram of random walk mobility model

图中"*"表示 25 个网关，每两个相邻网关之间相距 100m，每种颜色的曲线表示每个终端的移动路径。

终端的每次移动后，首先判断是否还与当前的网关相连接(判断标准为此时终端与当前连接的网关的距离是否超过 75m)，若已经与网关断开连接，则连接新的距离最近的网关，并判断是否与该网关有过连接，若有过连接，判断是否已经超过时间值 T，若未超过则保持原有的主配对密钥，否则形成新的配对密钥。

对时间 T 设置不同的数值，并考虑平均速度不同的情况，最终一天内 100 个终端需要形成的主配对密钥次数如图 9 所示。

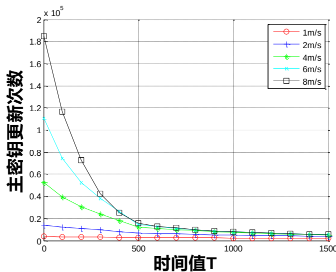


图 9 一天之内终端形成主配对密钥频率

Fig. 9 Frequency of the master pairing key formed by the terminal within one day

对于不同的时间值 T，当终端移动平均速度相同，一天之内加密密钥生成的次数趋于常数，其数值与当 T=0 时，主配对密钥生成次数基本一致。本文仿真四次不同速度下生成加密密钥频率如表 3 所示。

表 3 一天之内终端形成加密密钥频率

Tab. 3 The frequency of the encryption key formed by the terminal within one day

速度/m/s	第一次	第二次	第三次	第四次
1	3692	3658	3764	3638
2	14187	14220	14075	14056
4	52643	52730	52530	52729
6	110573	110508	110860	110599
8	185020	184935	185140	185464

由文献[6]可知，生成主密钥时间与能耗约为生成加密密钥时间与能耗的 2000 倍，所以在考虑安全性与能耗之间的权衡问题时，可以忽略加密密钥所需能耗的影响。

由图 8 可知，随着时间值 T 的增加，主密钥生成频率减少，且速度越大，主密钥频率减少幅度越大。这是由于速度越大，该终端在相同时间内移动的范围就越大，它能够在相应的时间值 T 内返回原网关通信范围的可能性就越大。

时间值 T 越大，主密钥更新频率越小，终端接入的安全性就会降低，但是所需能耗越小。图 8 曲线显示，在 0-500s 内，主密钥更新频率减少较快，500s 之后，减少速度趋于平缓。终端在保障安全性的同时还需要减少能量的损耗与时间的浪费，所以一般可以将时间值 T 设置为 500s。

5 结束语

现有的战术环境下的安全认证方案是在节点与核心网断开连接的前提下实施的，由于缺少云端作为计算能力强大的完全可信第三方，常规的终端可信接入算法难以实施。本文基于无证书密钥管理的安全接入方案较好地解决了此前方案中存在的缺少互相认证与信任托管的问题，而且详细地介绍了终端移动后可能产生的各种情况，分析了应对这些情况的处理方法，并且能够根据实际情况权衡能耗与安全性之间的关系。但是本文仍然存在一些缺点，如文中主要考虑的随机漫步模型不能完全反映战术环境中终端的移动情况。以后的工作可以综合考虑不同场景中对应的移动模型，并结合适当的算法，权衡安全性与能耗的关系，这样才能精确地计算不同环境下的 T 值；此外，本文对于受入侵节点的检测主要依赖主控节点较强大的入侵检测机制，以后的工作可以考虑通过节点之间互相监测的方式及时发现受损或收入侵的节点。

参考文献：

[1] Sha Kewei, Wei Wei, T. Yang A, *et al.* On security challenges and open issues in Internet of Things [J]. Future Generation Computer Systems,

2018, 83: 326–337.

[2] Kouicem D E, Bouabdallaha A, Lakhlef H. Internet of things security: A top-down survey. [J]. Computer Networks, 2018, 141: 199–221.

[3] Marianne R, Brannsten. Federated Single Sign On in Disconnected, Intermittent and Limited (DIL) Networks [C]// 81st IEEE Vehicular Technology Conference, Piscataway, NJ: IEEE Press, 2015: 1-5.

[4] Echeverr S, Lewis G A, Root J. Cyber-Foraging for Improving Survivability of Mobile Systems [C]// 34st Anuual IEEE Military Communications Conference, Piscataway, NJ: IEEE Press, 2015: 1421-1426.

[5] Echeverr, Grace A. Lewis, James Root. Secure VM Migration in Tactical Cloutlets [C]// 2017 IEEE Military Communications Conference, Piscataway, NJ: IEEE Press, 2017: 388-393.

[6] Al-Riyami S S, Paterson K G. Certificateless Public Key Cryptography [C]// 9th International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2003: 452-473.

[7] 郎晓丽，曹素珍，刘祥震，等. 具有高效授权的无证书公钥认证可搜索加密方案 [J]. 计算机工程与科学, 2020, 42 (03): 418-426. (Lang Xiaoli, Cao Suzhen, Liu Xiangzhen, *et al.* A Certificateless Public Key Authenticated Searchable Encryption Scheme With Efficient Authorization [J]. Computer Engineering and Science, 2020, 42 (03): 418-426.)

[8] Tedeschi P, Sciancalepore S, . Eliyan A, *et al.* LiKe: Lightweight Certifificateless Key Agreement for Secure IoT Communications [J]. IEEE Internet of Things Journel, 2020, 7 (1): 621-638.

[9] Khan M A, Ullah I, Nisar S. An Efficient and Provably Secure Certificateless Key-Encapsulated Signcryption Scheme for Flying Ad-hoc Network [J]. IEEE Access, 2020, 8, : 36807-36828.

[10] 赵楠，章国安. VANET 中基于无证书环签密的可认证隐私保护方案 [J]. 计算机科学, 2020, 47 (03): 312-319. (Zhao Nan, Zhang Anguo. Authenticated Privacy Protection Scheme Based On Certificateless Ring Signcryption In VANET [J]. Computer Science, 2020, 47 (03): 312-319.)

[11] Kalra S, Sood S K. Secure authentication scheme for IoT and cloud servers [J]. Persasive and Mobile Computing, 2015, 24: 210-223.

[12] Konlitz N. Elliptic curve cryptosystems [J]. Mathematics of Computation, 1987, 48 (177): 203-209.

[13] Wang K H, Chen C M, Fang W, *et al.* A secure authentication scheme for Internet of Things [J]. Pervasive and Mobile Computing, 2017, 42: 15-26.

[14] Chang C C, Wu H L, Sun C Y. Notes on"Secure authentication scheme for IoT and cloud servers" [J]. Pervasive and Mobile Computing, 2017, 38: 275-278.

[15] Echeverria S, Klinedinst D, Williams K. Establishing Trusted Identities in Disconnected Edge Environments [C]// 1st Symposium on Edge Computing, Piscataway, NJ: IEEE Press, 2016: 51-63.

[16] SHAMIRA. Identity-based cryptosystems and signature schemes [C]// Annual International Cryptology Conference, Berlin: Springer, 1984: 47-53.

[17] Boneh D, Franklin M. Identity-Based Encryption from the Weil Pairing [C]// 21st Anuual International Cryptology Conference, Berlin: Springer, 2001: 586-615.

[18] Pedersen T P. A Threshold Cryptosystem without a Trusted Party [C]// Proceedings of the 10th Annual International Conference, Berlin: Springer1991: 522-526.

[19] Echeverria S, Klinedinst D, Seitz L. Authentication and Authorization for IOT Devices in Disadvantage Environments [C]// World Forum on Internet of Things. Piscataway, NJ: IEEE Press, 2019: 368-372.

[20] Seo S H, Won J, Sultana S, *et al.* Effective Key Management in Dynamic Wireless Sensor Networks [J]. IEEE transactions on information forensics and security, 2015, 10 (2): 371-383.

[21] Seo S H, Won J, Bertino E. pCLSC-TKEM: a Pairing-free Certificateless Signcryption-tag Key Encapsulation Mechanism for a Privacy-Preserving IoT [J]. Transactions on Data Privacy, 2016, 9 (2): 101-130.

[22] Boneh D, Lynn B, Shacham H, Short signatures from the Weil pairing [J]. Journal of Cryptology, 2004, 17 (4): 297–319.

[23] ZhouCaixue, Zhao Zhiqiang, Wan Zhou, *et al.* Certificateless Key-Insulated Generalized Signcryption Scheme without Bilinear Pairings [J]. Security & Communication Networks, 2017, 2017: 1-17.

[24] Xiong Hu, Mei Qian, Zhao Yanan. Efficient and Provably Secure Certificateless Parallel Key-Insulated Signature Without Pairing for IIoT Environments [J]. IEEE Systems Journal, 2020, 14 (1) 310-320.

[25] Bellare, Mihir, Canetti: Keying Hash Functions for Message Authentication [M]. Advances in Cryptology — CRYPTO'96. Berlin: Springer, 1996.